Technical Cybersecurity

Cybersecurity Today: Advanced Persistent Threats

APT == Nation State

Advanced Persistent Threat

- Advanced, sophisticated malware
- First associated with Stuxnet
- Other campaigns identified as APT later

Professional, innovative malware

- New techniques and few mistakes
- Multiple 0-days, Targeted
- New persistence models

Overused Term

SOME THINGS ARE DEFINITELY APT

- Stuxnet, Duqu 2.0, Blackenergy

SOME THINGS ARE DEFINITELY NOT

- Almost all malware

Why not more?

APT is expensive

- Technical skill, targeting, resource acquisition, engineering

0-days are costly

- Can cost upwards of $500K (see: Zerodium)

Asset acquisition is risky

- Stuxnet used private keys acquired (read: stolen) from businesses

New approaches are expensive

- Code needs to be developed and tested v. representative systems

How did this all start?